REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated July 26, 2005. Claims 1-30 are pending. Claims 1-30 are rejected. Claims 1, 7, 16 and 22 have been amended. No claims have been canceled or added. Accordingly, claims 1-30 remain pending in the present application.

Claims 1, 7, 16 and 22 are rejected under 35 USC 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. The Examiner states that the "omitted structure cooperative relationships are present in limitation 'migrating the migratable keyblob from the computer to itself'. It is not clear where is the keyblob being migrated to."

Accordingly, Applicant has amended claims 1, 7, 16 and 22 to recite that the migratable keyblob is migrated from the computer to the security residing on the computer. Thus, amended claims 1, 7, 16, and 22 traverse the Examiner's rejection.

Claims 3, 7, 18, 22, and 24 are rejected under 35 USC 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. The Examiner states that the "limitation 'generating a ... random number by hashing the pass phrase' renders the instant claims indefinite, because hashing the pass phrase will not produce a random number. Based on the pass phrase and the hash function used the number produced will be definite and not random."

Applicant submits that it is known in the art that the hashing of a pass phrase provides a number with enough entropy to be considered "random". If there is at least 20 bytes of entropy in the pass phrase, then that entropy is distilled in the resultant hash. In support, Applicant directs the

Examiner to the technical report entitled "The Memorability and Security of Passwords – Some Empirical Results", by Yan et al., September 2000 (submitted herewith).

Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Oorschot (5,850,443) in view of Eldridge (6,061,799). The Examiner argues that Oorschot discloses "a key management system for mixed-trust environments (see abstract). Oorschot teaches that symmetric key is encrypted using asymmetric technique, and along with this transporting ciphertext derived form plaintext encrypted under this symmetric key (see abstract and Fig. 2)." The Examiner further argues: the limitations "creating a migratabale [sic] keyblob... wherein the migratable keyblob contains a key" is met by encrypted block of data having A and B headers (see Fig. 1); the limitations "wrapping the migratable keyblob with a public key of the key's parent key" is met by Fig. 1, depicting encryption of the symmetric key K by A and B public encryption keys; and the limitations "migrating the migratable keyblob" is met by sending the encrypted message with the headers from entity A (Fig. 3) to entity B (Fig. 4). The Examiner admits that Oorschot does not explicitly teach encrypting the random number with a pass phrase for a user, and cites Eldridge as teaching this limitation.

Applicant respectfully disagrees. The present invention, as recited in independent claims 1, 7, 16, 22, double encrypts keys. A key is subject to a first encryption by creating a migratable keyblob using a random number, where the migratable keyblob contains the key. The key is then subject to a second encryption layered on top of the first encryption by wrapping the migratable keyblob with a public key of the key's parent key. Thus, the same key has two layers of encryption. The random number is then encrypted with a pass phrase for a user of the key, and the encrypted random number is stored. The migratable keyblob is migrated from the computer to the secure chip residing within the computer.

Oorschot discloses a first party encrypting a cryptographic key of a cryptographic strength commensurate with the degree of trust of the environment in which the first party is located, by using a low trust encryption public key of the first party to generate a first party encrypted cryptographic key. The first party **separately** encrypts the cryptographic key using a high trust encryption public key of the second party to generate a second party encrypted cryptographic key, and concatenates the first and second encrypted cryptographic keys. (col. 4, lines 16-32)

However, in contrast to the present invention, for each encryption of the cryptographic key in Oorschot, the key is encrypted only once. Even after concatenation, the cryptographic keys are each encrypted only once.

Thus, Oorschot in view of Eldridge does not teach or suggest creating a migratable keyblob using a first random number, wherein the migratable keyblob contains a key, and wrapping the migratable keyblob with a public key of the key's parent key, in combination with the other elements, as recited in independent claims 1, 7, 16, and 22.

Therefore, for the above identified reasons, the present invention as recited in independent claims 1, 7, 16, and 22 is neither taught nor suggested by the cited references. Applicant further submits that claims 2-6, 8-15, 17-21, and 23-30 are also allowable because they depend on the above allowable base claims.

In view of the foregoing, Applicant submits that claims 1-30 are patentable over the cited references. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

October 26, 2005
Date

/Michele Liu/ Reg. No. 44,875
Michele Liu
Attorney for Applicant(s)
(650) 493-4540